

# Running your Cyber Security program as a Business

Manny Morales CISSP, CISM, CISA, CSM  
Office of the State Comptroller  
17<sup>th</sup> Annual New York State  
Cyber Security Conference  
June 4, 2014

# Why this approach

- ▶ Business owns the Data
- ▶ Businesses are willing to take more risk
- ▶ **IT** is still reactive, Businesses are more strategic
- ▶ Cyber Crime is increasing
- ▶ When security is viewed as an **IT** function, it has to compete with all other **IT** services
- ▶ Improves Management buy-in



# What are Business fundamentals

- ▶ The Customer
  - ▶ Profit and Loss
  - ▶ Marketing
  - ▶ Sales
  - ▶ Investment
  - ▶ Innovation of new ideas
  - ▶ Metrics – how well are you doing
- 
- ▶ These same principles can apply to Cyber security



# How to run like a business

- ▶ Need to know what your business is
- ▶ Need to know who is in charge and align with them
- ▶ Need to talk their language
- ▶ Need to understand their needs
- ▶ Get the right security talent to run your program
- ▶ Have a budget or access to funds



# Equate business terms to your Cyber Security program

- ▶ Who is the Customer – the business Owner and their clients
- ▶ Profit – Having a secured system that clients can trust
- ▶ Loss – preventing loss of data, recouping cost due to a breach. Use only examples that apply, don't mix government with private sector



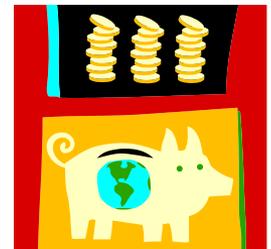
# Equate business terms to your Cyber Security program – con't

- ▶ Marketing – Getting business leaders on your side. Need to get business advocates
  - Get involved in the Governance process
- ▶ Salesmanship – Selling why security is good for the business and IT
  - Demonstrate that you Understand business risk



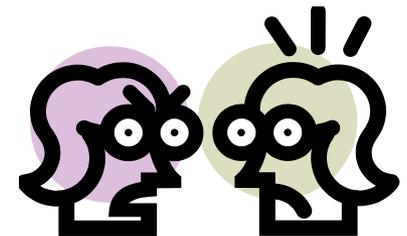
# Equate business terms to your Cyber Security program – con't

- ▶ Investment – creating an ROI, why the need to put \$\$ into the business to support security
- ▶ Metrics – measuring the success of your program – Use business metrics such as:
  - How quickly the business recovered from an incident
  - How many attacks were addressed



# Government or Private Sector

- ▶ Understand the difference – however, same principals hold
- ▶ In Government – protecting citizen's information, being efficient, getting elected, regulations
- ▶ In the Private Sector – protecting the brand, cost of doing business, reducing loss



CUSTOMER



CYBER SECURITY

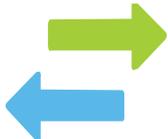


PAYROLL



IT

SECURITY OPERATIONS



# Security needs to break away from IT

- ▶ Security leaders need to assume a business position and attitude
- ▶ Cyber Security needs more focus on people and processes
- ▶ Educate the Business. IT is an enabler, not the total solution



# Need to meet with IT

- ▶ Build the business case for a business Cyber Security program model
  - Business drives IT
  - Businesses are getting more security educated, they want a 'Voice'
  - Businesses have Increased their presence on the Internet
  - Reaffirm that the Business owns the data



# How it Benefits IT

- ▶ Having a Business mentality helps get IT what they need
  - Allows security to be up front when business requirements are given to IT
  - Build more secured systems
  - Will dispel the idea that security is an IT function
- ▶ Engaging the Business first, allows for better IT integration in security operations
- ▶ IT needs to focus more on Operational security



# What Security Framework do I use

- ▶ COBIT 5 – from ISACA
  - ▶ SANS “20” Critical Controls
  - ▶ PCI
  - ▶ HIPAA and HITECH
  - ▶ NIST – Infrastructure Cyber Security
  - ▶ ISO 27000
- ▶ *Think about what you are trying to accomplish?*

Protect

Monitor

Recover



# Two parts to a Cyber Security program

- ▶ The Cyber Security Program – The People and Process
  - What Businesses care about
- ▶ The Security Operations program – The IT side
  - What IT is chartered to do; protect the infrastructure
- ▶ Before you can even think in business terms, separate the two; however, still need to partner together



# A Cyber Security program

## ▶ Basic elements

- Policies, Hardening guidelines, security standards
- Awareness
- Data Classification
- Security Architecture – Secure System Development Lifecycle
- Risk Management
- Compliance and Audit
  - Vulnerability and Penetration Testing
  - Privilege User Management
  - Monitoring and Reporting – Metrics
  - Incident Response



# An IT Operations Security program

- ▶ Focus is on
  - Provisioning and audits
  - Patch Management
  - Monitoring
  - SW and HW reviews
  - Network certifications and reviews
  - Risk assessments
  - Performing Intrusion testing (scanning)
- ▶ Address this as a need for sound infrastructure protection



# The Challenges

- ▶ **IT** does not want to let go
- ▶ How to talk the business language
- ▶ Not having a business advocate –Building trust
  
- ▶ Attaining Security talent
- ▶ Having a Budget
  
- ▶ Takes time to implement



# The Rewards

- ▶ Business leaders and Management will stand by you – “Strength in Numbers”
- ▶ Better protection for Data and the Application
- ▶ IT will get better requirements
  
- ▶ Cyber Security will be embedded into the Business
- ▶ Security will no longer be an afterthought





How to contact me:  
[mmorales@osc.state.ny.us](mailto:mmorales@osc.state.ny.us)

